

## Fortinet Solutions RSSO (RADIUS Single Sign On)

Author: David Oliver  
Consulting Systems Engineer

### Contents

<b>Introduction .....</b>	<b>3</b>
<b>Deployment Considerations .....</b>	<b>3</b>
<b>Requirements .....</b>	<b>3</b>
<b>RADIUS Accounting Direct to Fortigate (Fortigate RSSO) .....</b>	<b>4</b>
Steps and related CLI / Configuration Example .....	5
Monitoring and Troubleshooting Examples.....	9
<b>RADIUS Accounting via FortiAuthenticator to Fortigate (FortiAuthenticator RSSO to FSSO) ...</b>	<b>12</b>
FortiAuthenticator Steps and related CLI / Configuration Example .....	13
FortiGate Steps and related CLI / Configuration Example .....	16
Monitoring and Troubleshooting Examples.....	19
<b>RADIUS Accounting via FortiAuthenticator RADIUS Accounting Proxy to Fortigate .....</b>	<b>23</b>
<b>(FortiAuthenticator RSSO to RSSO) .....</b>	<b>23</b>
FortiAuthenticator Steps and related CLI / Configuration Example .....	24
FortiGate Steps and related CLI / Configuration Example .....	26
<b>Related Information .....</b>	<b>27</b>

## Change Log

Revision	Date	Change Description	Owner
1	2014-07-21	Initial Release	David Oliver

## Introduction

FortiGate and FortiAuthenticator support the use of RADIUS Start, Stop, and Interim Update messages to authenticate and manage active users transparently. Carriers often use RADIUS servers tied into backend billing systems to record usage information. Enterprises often use RADIUS servers to authenticate VPN connections.

In both cases, the entities in question may want to provide UTM functions or other traffic restrictions to this traffic without having the user re-enter their credentials. Fortinet RSO solutions can assist in deploying these solutions.

## Deployment Considerations

The following are important aspects that need to be considered prior to using RSO:

- RADIUS environment needs to be configured to send accounting records. How to configure every possible RADIUS server is beyond the scope of this document.
- For direct to Fortigate RSO, RADIUS server needs to be configured with appropriate group names and users added to them.
- For RADIUS to FAC to FSO, Your LDAP Directory needs to be configured with appropriate group names and users added to them.
- It is no longer necessary to import or utilize the Fortinet VSA dictionary

We use the following default RADIUS attributes in Fortigate

User-Name (the username that logged in)

Class (use this for the group name)

Framed-IP-Address (the ip the user logged in from)

We use the following default RADIUS attributes in FortiAuthenticator

User-Name (the username that logged in)

Framed-IP-Address (the ip the user logged in from)

Fortinet-Group-Name (use this for the group name.)

{Group attribute is not entirely necessary as FAC will figure it out by querying the LDAP directory}

## Requirements

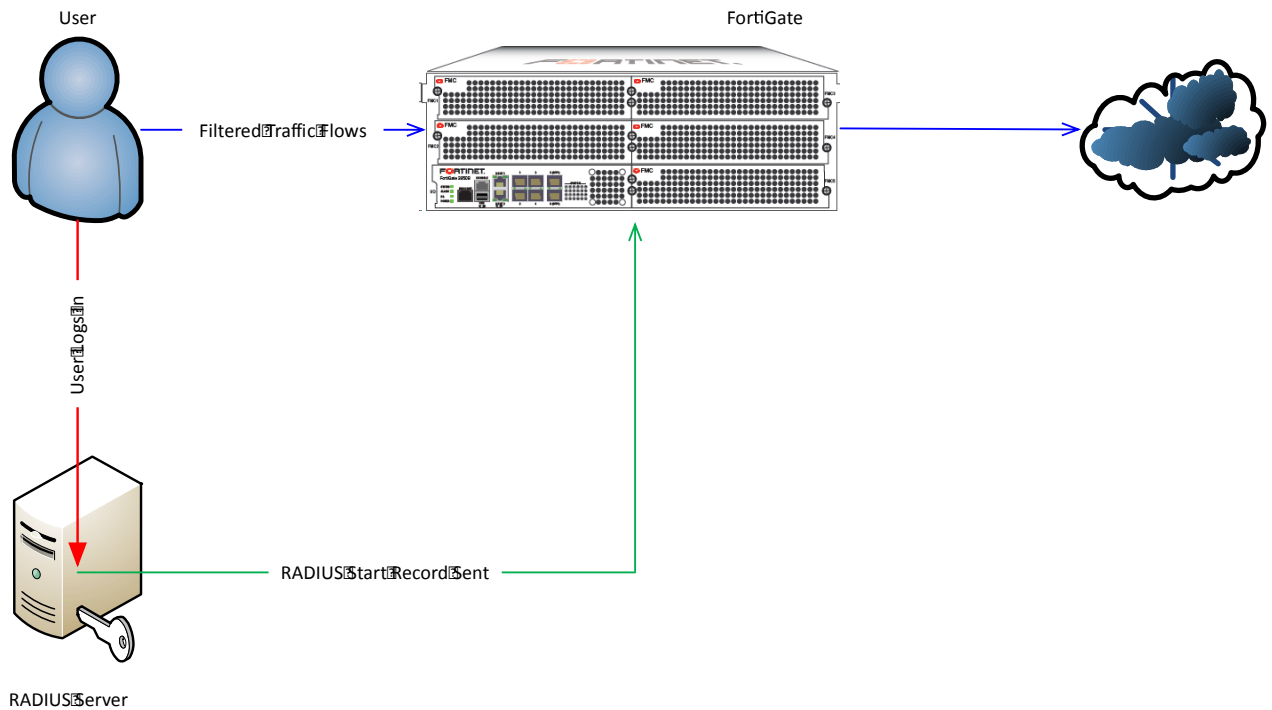
FortiOS 5.0.6. This configuration example uses FortiOS 5.0.6 and FortiAuthenticator 3.0.1.

Creation of RADIUS Accounting Records was performed using NTRADping.

## RADIUS Accounting Direct to Fortigate (Fortigate RSSO)

FortiOS supports the use of RADIUS Start, Stop, and Interim Update messages to authenticate and manage active users transparently. Configuration of the Fortigate to receive and utilize these records is quite straight forward.

Diagram



## Steps and related CLI / Configuration Example

### Step 1 – Configure Interface to receive RADIUS Accounting Records

It is required that at least one interface that can be reached by the RADIUS Server is configured to listen for RADIUS Accounting messages.

Figure 1 – Configure interface CLI.

```
edit "port4"
set vdom "root"
set ip 10.2.2.254 255.255.255.0
set allowaccess ping radius-acct
set type physical
set explicit-web-proxy enable
set alias "VMNet4"
set snmp-index 4
next
```

Figure 2 – Configure interface GUI.

**FortiGate VM64**

**Edit Interface**

Name: port2(00:0C:29:75:FC:39)  
 Alias: Inside\_VMNet1  
 Link Status: Up  
 Type: Physical Interface  
 Virtual Domain: root

Addressing mode: ☒ Manual ☐ DHCP ☐ Dedicate to FortiAP  
 IP/Network Mask: 172.16.245.132/255.255.255.0  
 IPv6 Address: ::0

Administrative Access: ☒ HTTPS ☒ PING ☐ HTTP ☒ FMG-Access ☐ CAPWAP  
☒ SSH ☒ SNMP ☐ TELNET ☐ FCT-Access

IPv6 Administrative Access: ☐ HTTPS ☐ PING ☐ HTTP ☐ FMG-Access ☐ CAPWAP  
☐ SSH ☐ SNMP ☐ TELNET

DHCP Server: ☐ Enable

Security Mode: None

Device Management  
 Detect and Identify Devices: ☐

Enable Explicit Web Proxy: ☒  
 Listen for RADIUS Accounting Messages: ☒  
 Secondary IP Address: ☐

Comments: Write a comment... 0/255

Administrative Status: ☒ Up ☐ Down

OK Cancel

## Step 2 – Configure RSSO Agent

Only one RSSO agent is configurable per VDOM. Since the RSSO agent can receive records from any RADIUS server configured to send records to it, more than one is not required to receive from multiple RADIUS servers.

The RADIUS server must be configured to send the following Attributes in the Accounting Start, Accounting Stop and Interim Update messages

User-Name (the username that logged in)

Class (The Fortigate uses this to determine the User Group name, Can be any attribute of type octetstring but “sso-attribute” must be set to whatever value you choose. )

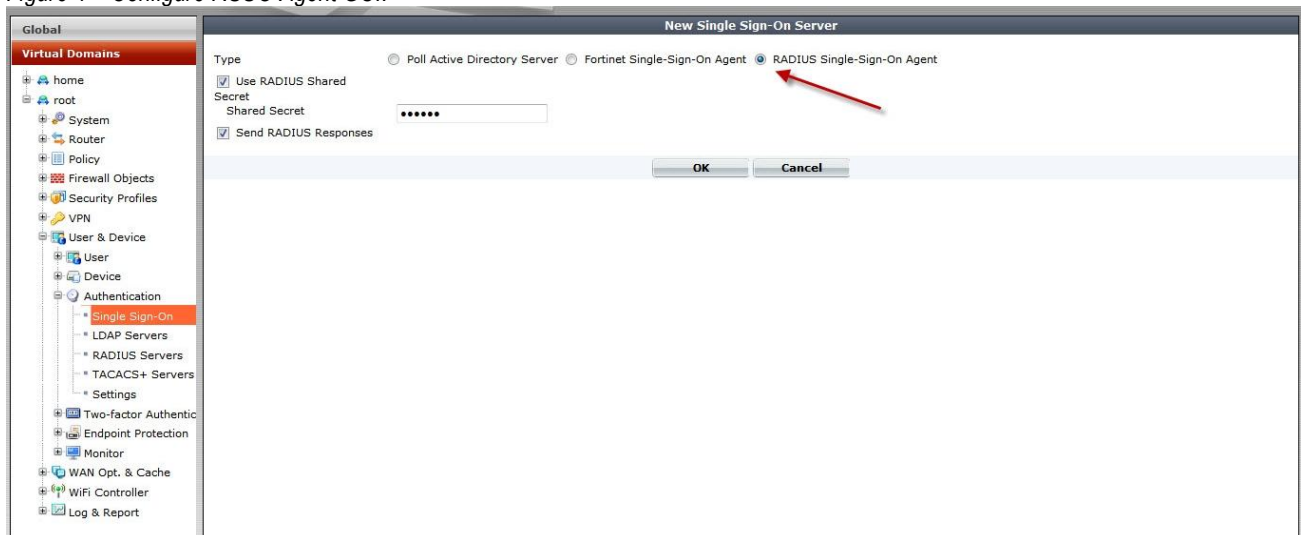
Framed-IP-Address (the ip the user logged in from)

These are standard RADIUS Attributes so the use of the Fortinet VSA Dictionary is not necessary

Figure 3 – Configure RSSO Agent CLI.

```
config user radius
edit "RSSO_Agent"
set rso enable
set rso-radius-response enable
set rso-endpoint-attribute User-Name
next
end
```

Figure 4 – Configure RSSO Agent GUI.



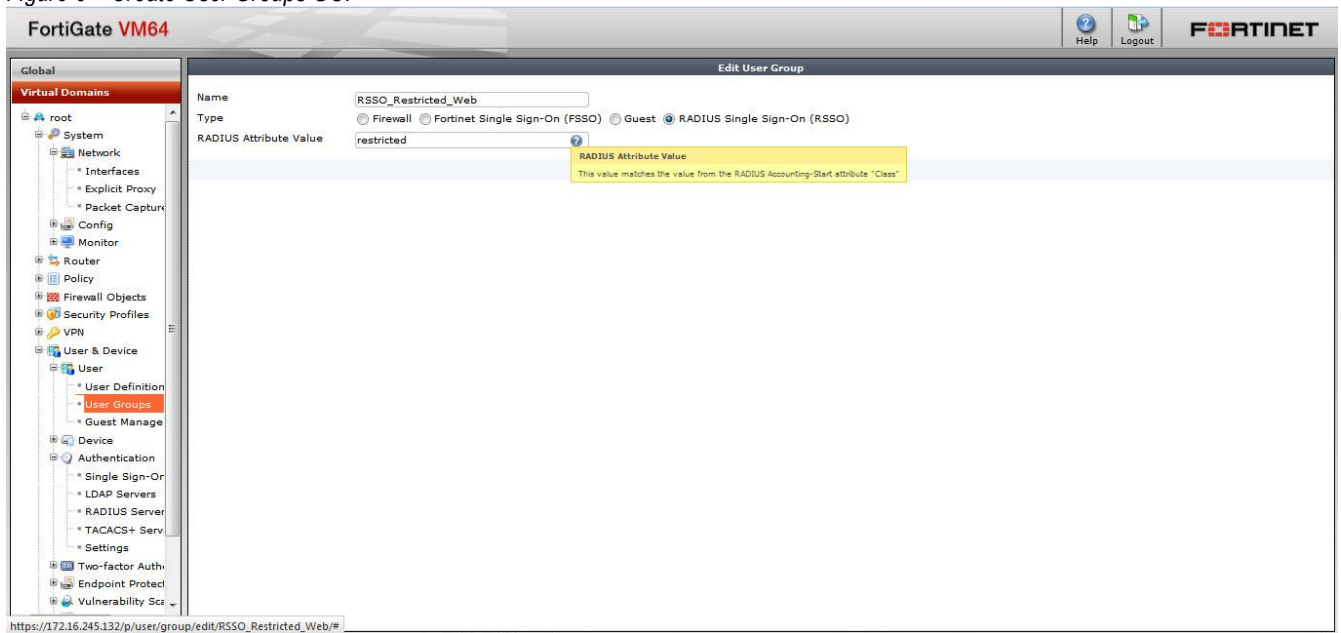
## Step 3 – Create User Groups

You will need to create User Groups for each class of user you want to authenticate. The RADIUS Attribute value is configured to match the Accounting Record value in the Attribute [Class].

Figure 5 – Create User Groups CLI

```
config user group
  edit "RSSO_Restricted_Web"
    set group-type rso
    set sso-attribute-value "restricted"
  next
  edit "RSSO_Unrestricted_Web"
    set group-type rso
    set sso-attribute-value "unrestricted"
  next
end
```

Figure 6 – Create User Groups GUI



## Step 4 – Configure Content Filter (if needed)

Refer to <http://docs.fortinet.com> for information on how to configure a content filter profile.

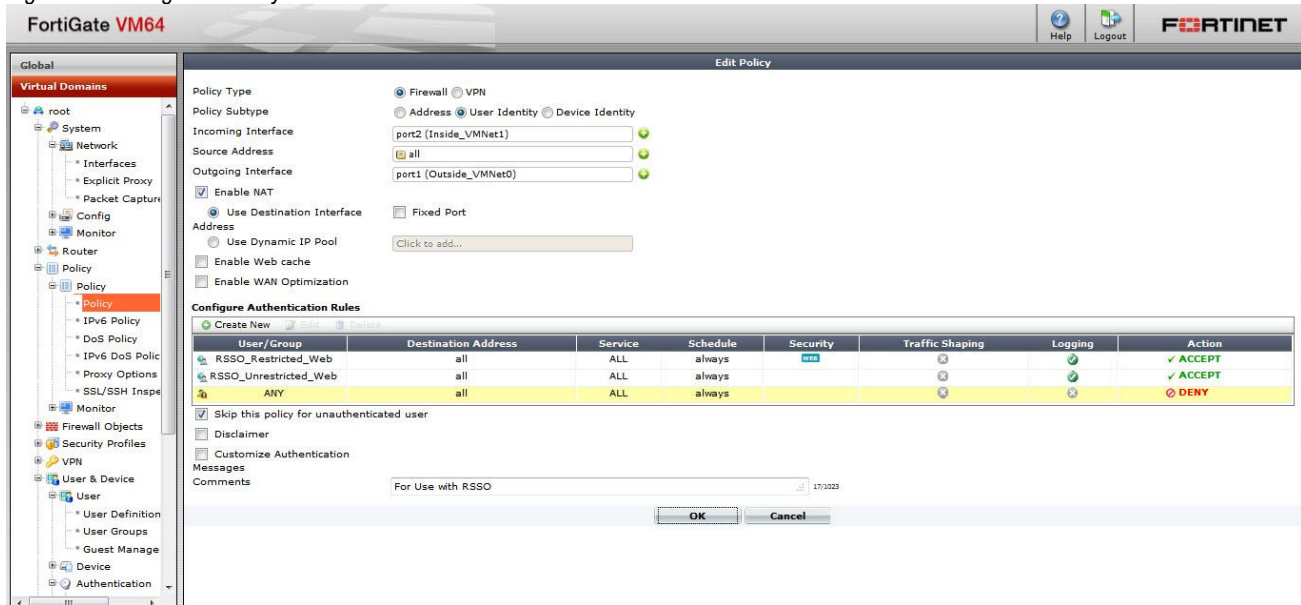
## Step 5 – Configure Identity Based Firewall Policies

*Figure 7 – Configure Identity Based Firewall Policies CLI*

```
config firewall policy
  edit 1
    set srcintf "port2"
    set dstintf "port1"
    set srcaddr "all"
    set action accept
    set rso enable
    set fall-through-unauthenticated enable
    set comments "For Use with RSSO"
    set identity-based enable
    set nat enable
    config identity-based-policy
      edit 1
        set schedule "always"
        set logtraffic all
        set utm-status enable
        set groups "RSSO_Restricted_Web"
        set dstaddr "all"
        set service "ALL"
        set webfilter-profile "restricted"
        set profile-protocol-options "default"
      next
    edit 2
      set schedule "always"
      set logtraffic all
      set groups "RSSO_Unrestricted_Web"
      set dstaddr "all"
      set service "ALL"
    next
  end
next
```

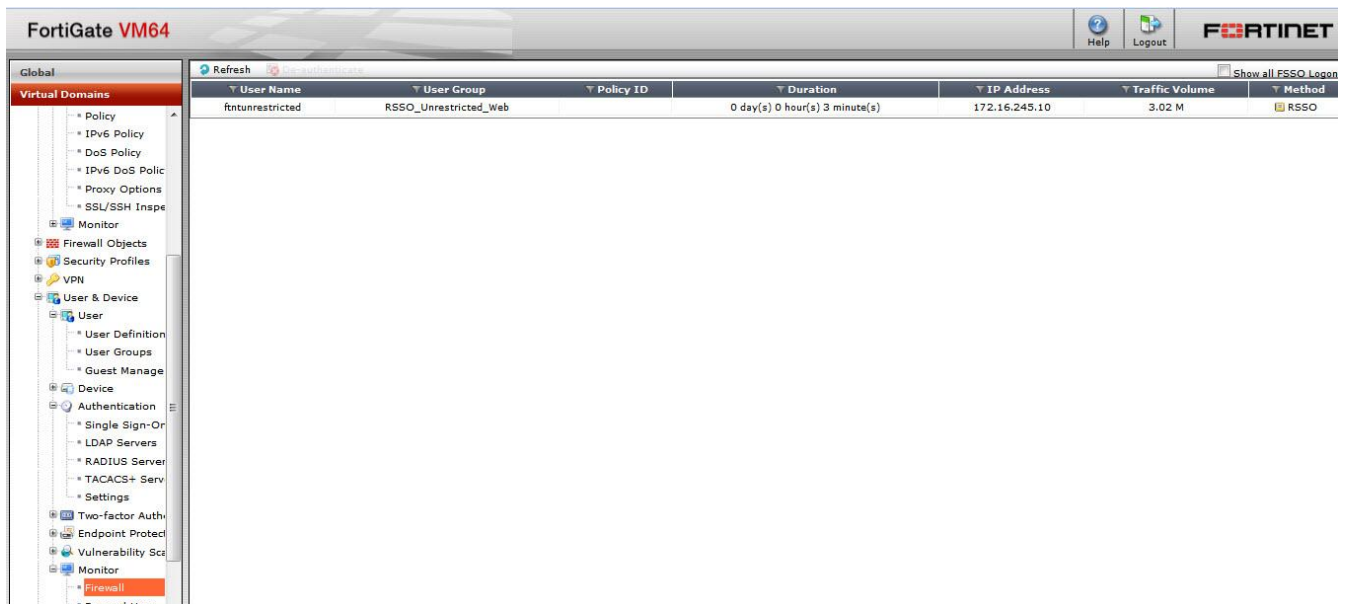


Figure 8 – Configure Identity Based Firewall Policies GUI



## Monitoring and Troubleshooting Examples

Figure 9 – Monitor Logged in Users GUI



You CANNOT deauthenticate a user via the GUI. It can only be done via CLI via the command “diag radiusd test 2”. This however will clear the RADIUS database of all RSSO users. To clear an individual user requires sending an Accounting Stop record for that user.

There are several commands in the CLI to monitor and query logged on users.

Figure 9 – Query Logged in Users CLI

diag rso query

allows you to query the rso database by

- carrier-endpoint Query by End Point. (this is the equivalent of the User-name)
- ip Query by IP address.(this is the Framed-IP address(es). This should be the host ip address
- rso-key Query by RSSO key. (this is the Class Attribute and relates to the Fortigate User Group name).

```
FortiGate-VM64-2 (global) # diag rso query ip 172.16.245.10
Querying IP '172.16.245.10'
Endpoint: ftntunrestricted
RSSO Key: unrestricted
IP Addresses:
    IP: 172.16.245.10, Time left (hh:mm:ss): 07:53:50 **
```

It is useful when you want to quickly look up who is at an IP, or list all the users in a specific Class (User Group) that are logged on.

Figure 10 – Query Logged in Users CLI and clear database

diag test app radiusd

allows you to query or clear the entire RADIUS database

Radius Daemon Test Usage:

-----

- 2 : Clear RADIUS server database
- 3 : Show RADIUS server database
- 33 : Show RADIUS server database (with start time)
- 4 : Show RADIUS server database info
- 9 : Check HA context table checksums
- 11 : Show HA sync connection status
- 20 : Show RADIUS server configuration cache
- 21 : Show RADIUS server interface configuration cache
- 99 : Restart

```
FortiGate-VM64-2 (global) # FortiGate-VM64-2 (global) # diag test app radiusd 3
RADIUS server database [vd root]:
"index","time left","ip","endpoint","block status","log status","profile group","ref count","use default profile"
1,07:49:59,"172.16.245.10","ftntunrestricted","allow","no log","unrestricted",1,No

FortiGate-VM64-2 (global) # diag test app radiusd 33
RADIUS server database [vd root]:
"index","start time","time left","ip","endpoint","block status","log status","profile group","ref count","use default profile"
1,1395866035,07:49:56,"172.16.245.10","ftntunrestricted","allow","no log","unrestricted",1,No

FortiGate-VM64-2 (global) # diag test app radiusd 4
RADIUS server database info [vd root DB 0 ID 0]:
Database Lock Count: 0
Endpoint Entries (now/max/total): 1/1/2
IP Address Entries (now/max/total): 1/1/2
Missed RADIUS Accounting-Stop: 0
Missed RADIUS Accounting-Start: 0
Lock Queue Length (now/max/total): 0/0/0
```

Figure 11 – debug RADIUS events as they occur

diag debug enable  
diag debug app radiusd -1  
allows you to debug RADIUS events as they occur

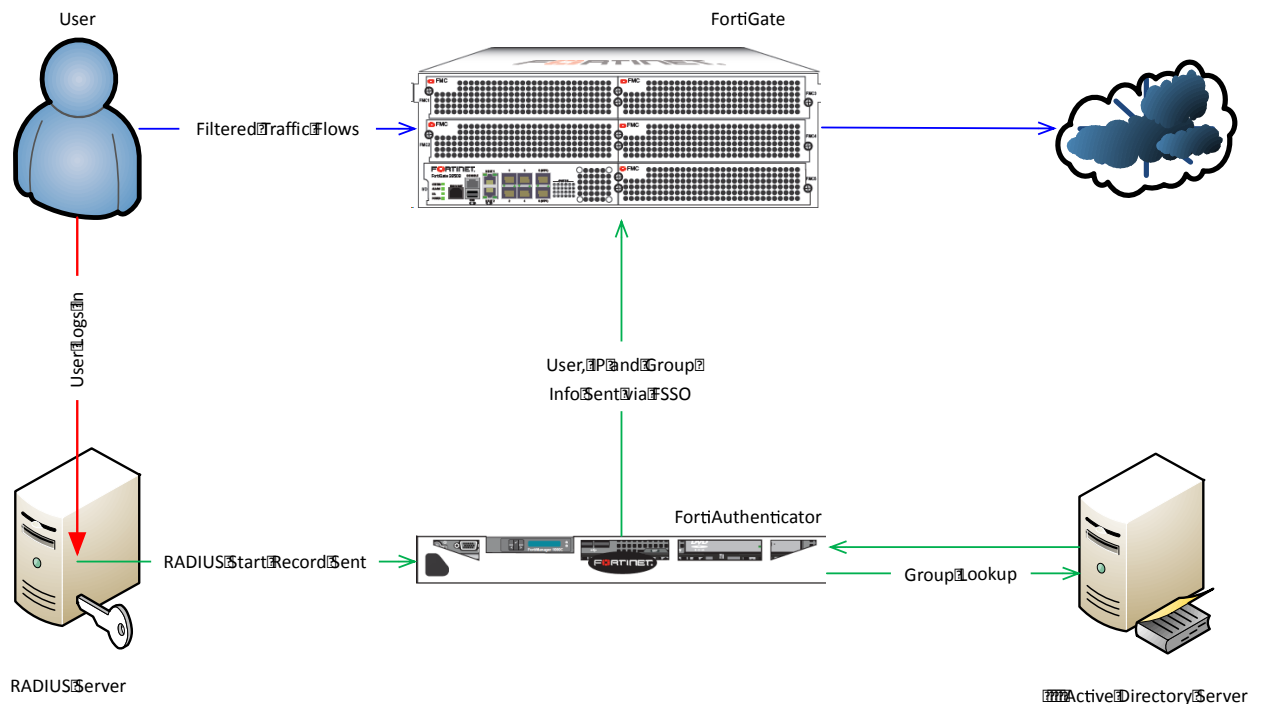
```
FortiGate-VM64-2 (global) # diag debug app radiusd -1
FortiGate-VM64-2 (global) # diag debug en
FortiGate-VM64-2 (global) # DB 0 insert [ep='ftntrestricted' pg='restricted' ip='172.16.245.10'] success
DB 0 insert [ep='ftntrestricted' pg='restricted' ip='172.16.245.10'] success
DB 0 insert [ep='ftntrestricted' pg='restricted' ip='172.16.245.10'] success
vd 0:root Remove auth logon for IP 172.16.245.10 for user ftntrestricted
vd 0:root Add/Update auth logon for IP 172.16.245.10 for user ftntunrestricted
DB 0 insert [ep='ftntunrestricted' pg='unrestricted' ip='172.16.245.10'] success
vd 0:root Add/Update auth logon for IP 172.16.245.15 for user ftntunrestricted
DB 0 insert [ep='ftntunrestricted' pg='unrestricted' ip='172.16.245.15'] success
vd 0:root Remove auth logon for IP 172.16.245.10 for user ftntunrestricted
vd 0:root Add/Update auth logon for IP 172.16.245.10 for user ftntrestricted
DB 0 insert [ep='ftntrestricted' pg='restricted' ip='172.16.245.10'] success
```

## RADIUS Accounting via FortiAuthenticator to Fortigate (FortiAuthenticator RSSO to FSSO)

FortiAuthenticator supports the use of RADIUS Start, Stop, and Interim Update messages to authenticate and manage active users transparently. It receives RADIUS accounting messages, Performs lookups against the LDAP server for Group Membership and then populates its FSSO cache with the correct information. This is then sent to the Fortigate as an FSSO login.

This is useful when Group membership information is handled by Active Directory or the RADIUS server is business-critical IT infrastructure, limiting the changes that can be made to the server configuration.

Diagram



## FortiAuthenticator Steps and related CLI / Configuration Example

### Step 1 – Configure FortiAuthenticator as an FSSO Collector Agent

FSSO must already be configured between the FortiAuthenticator and the Fortigate(s)

For information on how to configure FortiAuthenticator for FSSO see <http://docs-legacy.fortinet.com/auth/3-0-0/FAC-3.0-Admin-Guide.pdf>

### Step 2 – Configure remote LDAP server

Figure 11 – Configure Remote Auth Server

The screenshot shows the FortiAuthenticator web interface. The top bar indicates 'Logged in as admin' and includes 'Help' and 'Logout' links. The left sidebar shows the 'System' menu expanded, with 'Authentication' selected. The main content area is titled 'Edit Remote LDAP Server'. It contains the following fields and sections:

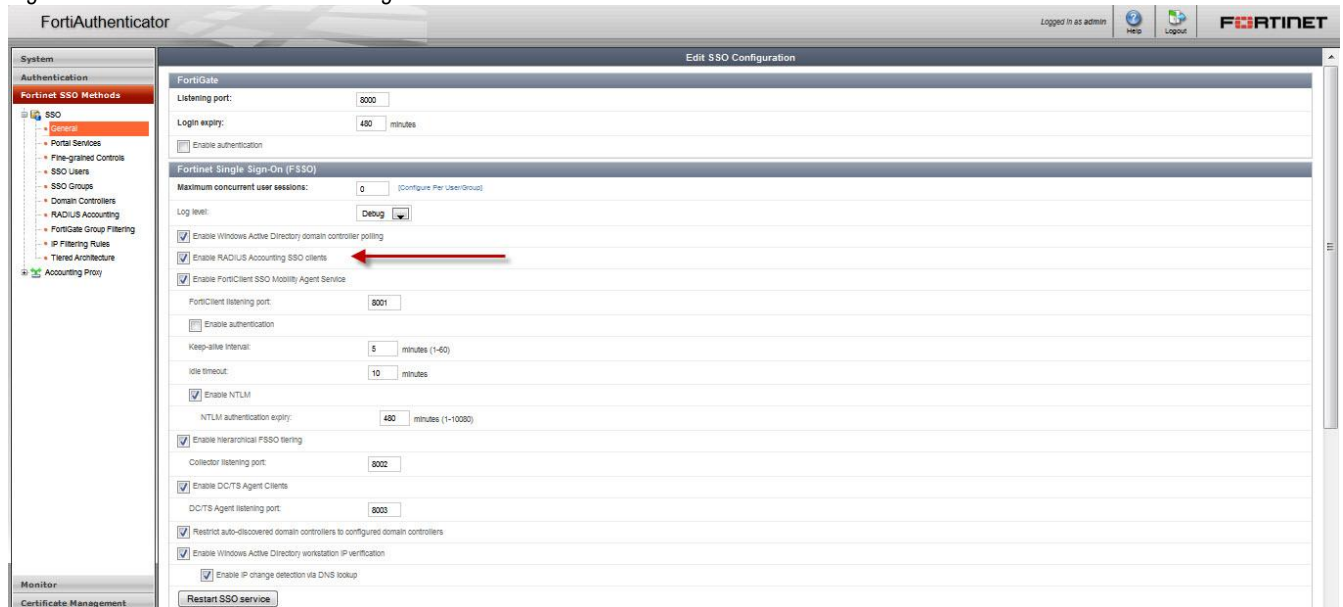
- Name:** FTNT-AD
- Server name/IP:** 172.16.248.12
- Port:** 389
- Base distinguished name:** DC=ftnt,DC=local
- Bind type:** Simple (selected), Regular
- Username:** cn=Administrator,cn=Users,dc=ftnt,dc=local
- Password:** [masked]
- User object class:** person
- Username attribute:** sAMAccountName
- Group membership attribute:** memberOf
- Secure Connection:** [checkbox] Enable
- Windows Active Directory Domain Authentication:**
  - [checkbox] Enable
  - Kerberos realm name:** FTNTLOCAL
  - Domain NetBIOS name:** FTNT
  - FortiAuthenticator NetBIOS name:** FortiAuthentic
  - Administrator username:** ftntAdministrator
  - Administrator password:** [masked]
- Remote LDAP Users:**

Username	Token	Actions
ftntrestricted		[edit] [delete]
ftntrestricted		[edit] [delete]
doilver		[edit] [delete]

At the bottom, there is an 'Import Users' button and 'OK'/'Cancel' buttons.

### Step 3 – Enable FSSO and RADIUS accounting SSO Clients

Figure 12 – Enable RADIUS accounting SSO Clients



## Step 4 – Configure RADIUS Accounting SSO Client

LDAP server must be selected from the drop-down list.

RADIUS Attributes

Username Attribute (default User-Name)

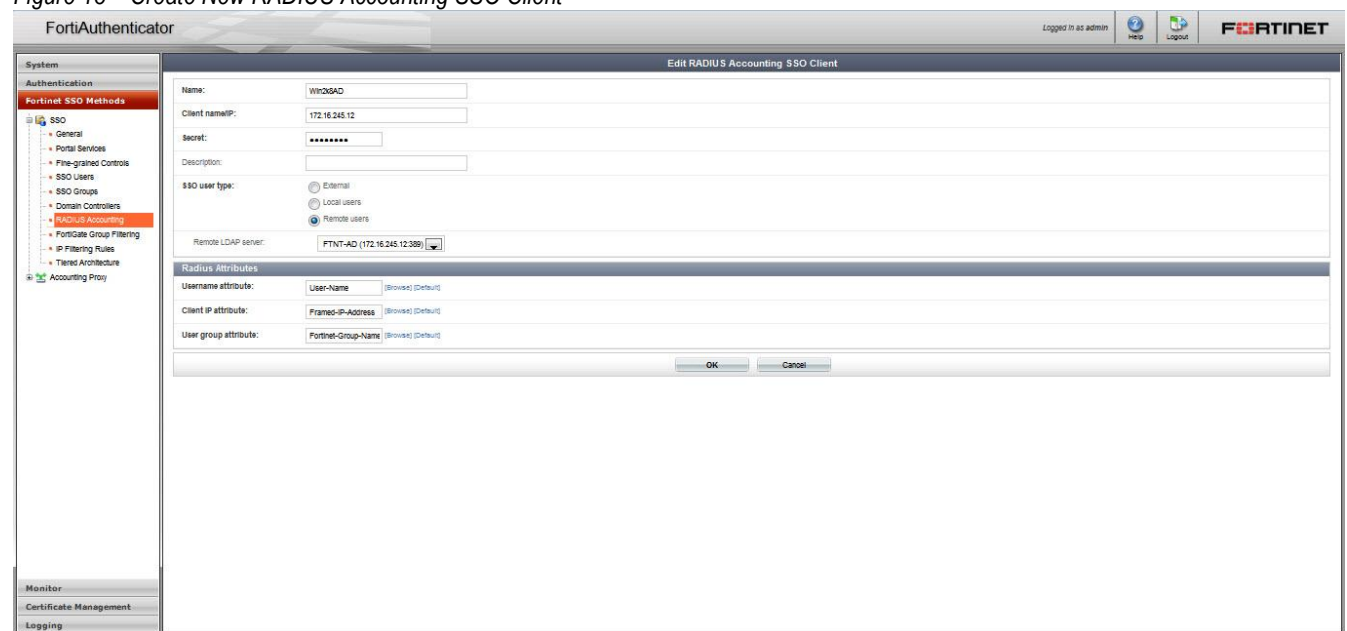
Client IP attribute (default Framed-IP-Address)

are required. I recommend leaving at the defaults.

User group attribute is not required.

The LDAP server created earlier must be selected from the drop-down list as this is how the FortiAuthenticator establishes group membership.

Figure 13 – Create New RADIUS Accounting SSO Client



FortiAuthenticator

Logged in as admin

Help Logout

System

Authentication

Fortinet SSO Methods

SSO

General

Portal Services

Fine-grained Controls

SSO Users

SSO Groups

Domain Controllers

RADIUS Accounting

FortiGate Group Filtering

IP Filtering Rules

Trusted Architecture

Accounting Policy

Monitor

Certificate Management

Logging

Edit RADIUS Accounting SSO Client

Name: WIDQAD

Client name/IP: 172.16.245.12

Secret: \*\*\*\*\*

Description:

SSO user type:

External

Local users

Remote users

Remote LDAP server: FTNT-AD (172.16.245.12389)

RADIUS Attributes

Username attribute: User-Name (Browse) (Default)

Client IP attribute: Framed-IP-Address (Browse) (Default)

User group attribute: Fortinet-Group-Name (Browse) (Default)

OK Cancel

## FortiGate Steps and related CLI / Configuration Example

### Step 1 – Configure FortiAuthenticator as an FSSO collector agent

Figure 14 – Configure FSSO agent CLI

```
config user fsso
  edit "FAC"
    set server "172.16.245.5"
  next
end
```

Figure 15 – Configure FSSO agent GUI

The screenshot displays the FortiGate VM64 GUI. On the left, the 'Global' menu is expanded, showing 'Virtual Domains' and 'Authentication'. Under 'Authentication', 'Single Sign-On' is selected. The main panel is titled 'Edit Single Sign-On Server'. It contains the following fields and options:

- Name:** FAC
- Primary Agent IP/Name:** 172.16.245.5
- Secondary Agent IP/Name:** (empty)
- Password:** (empty)
- LDAP Server:** Click to set...
- Users/Groups:** View Users/Groups (selected), Edit Users/Groups
- Users/Groups List:** UNRESTRICTEDWEB, RESTRICTEDWEB
- Buttons:** Apply & Refresh, OK, Cancel

Make certain to select groups.

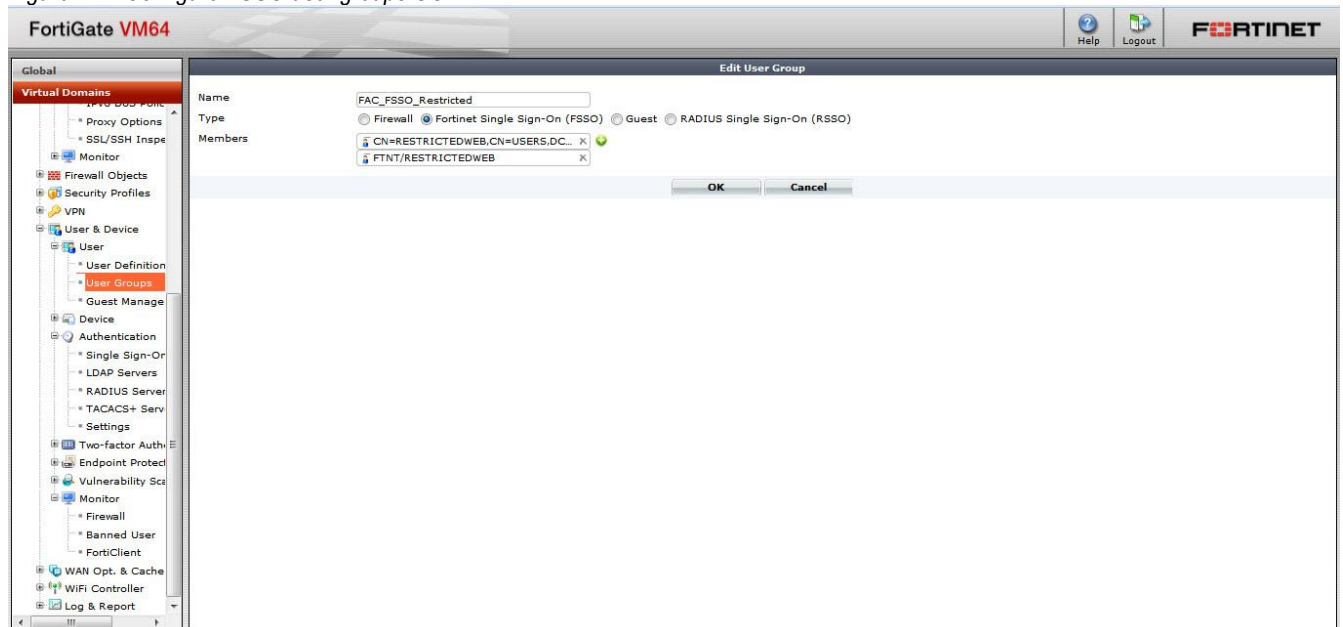


## Step 2 – Configure FSSO User Groups

Figure 16 – Configure FSSO user groups CLI

```
config user group
edit "FTNT_FSSO_RestrictedUsers"
set group-type fsso-service
set member "FTNT/RESTRICTEDWEB"
next
edit "FTNT_FSSO_UnRestrictedUsers"
set group-type fsso-service
set member "FTNT/UNRESTRICTEDWEB"
next
end
```

Figure 17 – Configure FSSO user groups GUI



## Step 3 –Configure Content Filter (if needed)

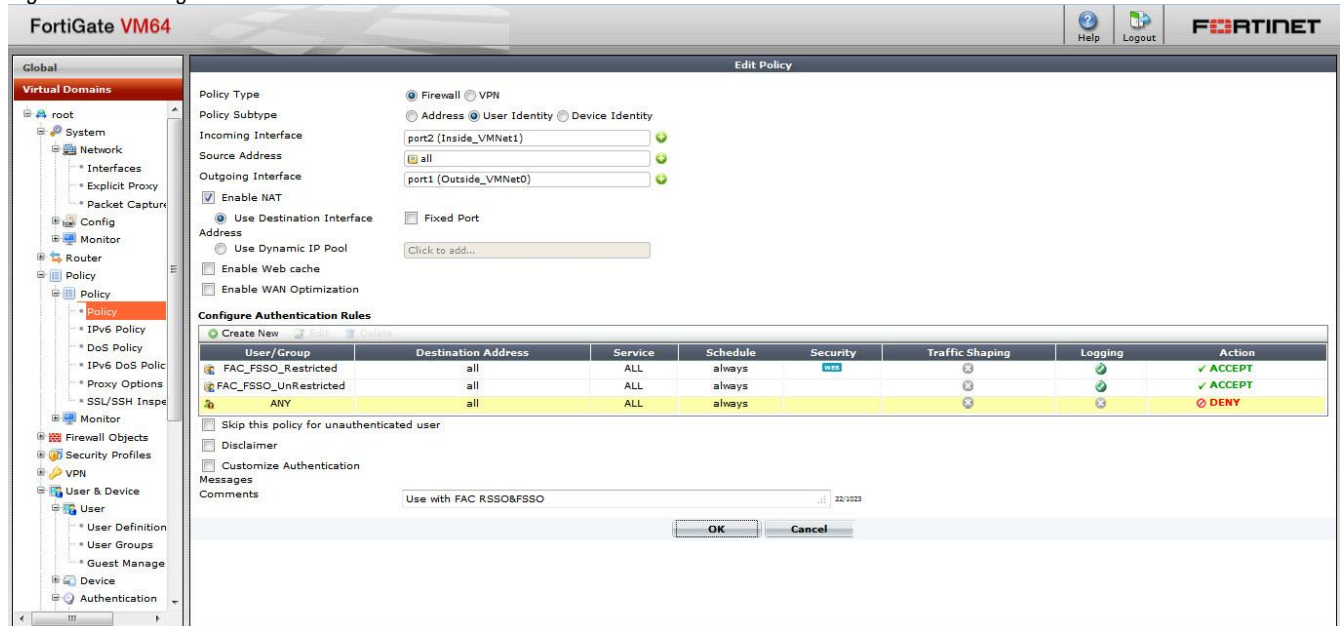
Refer to <http://docs.fortinet.com> for information on how to configure a content filter profile.

## Step 4 – Configure Identity Based Firewall Policies

Figure 17 – Configure Firewall Policies CLI

```
config firewall policy
edit 2
    set srcintf "port2"
    set dstintf "port1"
    set srcaddr "all"
    set action accept
    set status disable
    set fsso enable
    set comments "Use with FAC RSSO&FSSO"
    set identity-based enable
    set nat enable
    config identity-based-policy
    edit 1
        set schedule "always"
        set logtraffic all
        set utm-status enable
        set groups "FAC_FSSO_Restricted"
        set dstaddr "all"
        set service "ALL"
        set webfilter-profile "restricted"
        set profile-protocol-options "default"
    next
    edit 2
        set schedule "always"
        set logtraffic all
        set groups "FAC_FSSO_UnRestricted"
        set dstaddr "all"
        set service "ALL"
    next
end
next
end
```

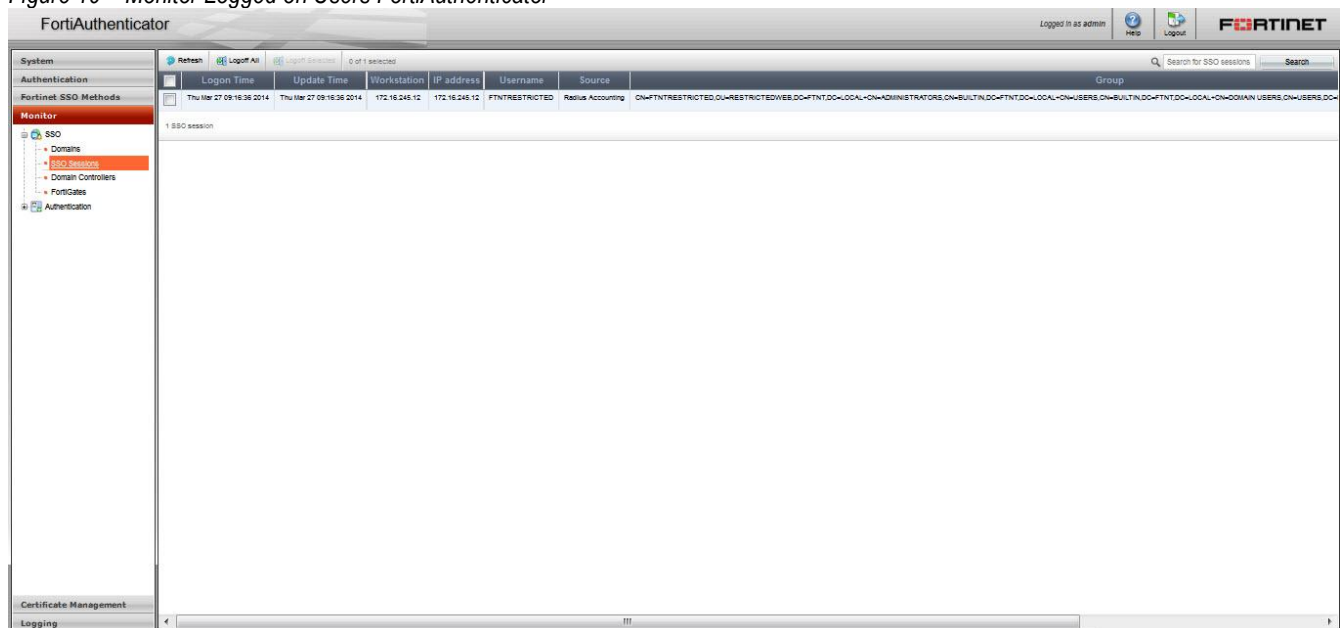
*Figure 18 – Configure Firewall Policies GUI*



## Monitoring and Troubleshooting Examples

There is little in the way of troubleshooting on the FortiAuthenticator. The Monitor/SSO Sessions is the only way to determine who is logged on from where.

Figure 19 – Monitor Logged on Users FortiAuthenticator



A single user can be deauthenticated on the FortiAuthenticator.

The Fortigate provides more troubleshooting tools for comprehensive debugging

Figure 20 – Monitor Logged on Users Fortigate GUI

User Name	User Group	Policy ID	Duration	IP Address	Traffic Volume	Method
FTNRESTRICTED	FAC_FSSO_Restricted		0 day(s) 0 hour(s) 20 minute(s)	172.16.245.12	N/A	FSSO

You cannot deauthenticate an FSSO user from the Fortigate GUI.

Figure 21 – Monitor Logged on Users Fortigate CLI

`diag debug authd fssso`

allows you to query, clear, list and provide comprehensive information about the status of FSSO sessions. It supports filtering which makes searching through thousands of potential logins quite simple.

FortiGate-VM64-2 (global) # `diag debug authd fssso`

`clear-logons` Clear logon information.

`filter` Filters used for list or clear logons.

`list` List current logons.

`refresh-groups` Refresh group mappings.

`refresh-logons` Resync logon database.

`server-status` Show FSSO agent connection status.

`summary` Summary of current logons.

FortiGate-VM64-2 (global) # `diag debug authd fssso filter`

`clear` Clear all filters.

`group` Group name.

`server` FSSO agent name.

`source` Source IP address.

`user` User name.

diag debug authd fsso list

*Unfiltered*

```
FortiGate-VM64-2 (global) # diag debug authd fsso list
----FSSO logons----
IP: 172.16.245.12  User: FTNTRESTRICTED  Groups: CN=RESTRICTEDWEB,CN=USERS,DC=FT
NT,DC=LOCAL  Workstation: 172.16.245.12  MemberOf: FAC_FSSO_Restricted
Total number of logons listed: 1, filtered: 0
----end of FSSO logons----
```

diag debug authd fsso filter user FTNTUNRESTRICTED

diag debug authd fsso list

*Filtered*

```
FortiGate-VM64-2 (global) # diag debug authd fsso filter user FTNTRESTRICTED

FortiGate-VM64-2 (global) # diag debug authd fsso list
----FSSO logons----
Total number of logons listed: 0, filtered: 1
----end of FSSO logons----
```

You can deauthenticate a single FSSO user from the CLI using

diag debug authd fsso filter user <username>

diag debug authd fsso clear

Figure 22 – debug AUTHD events as the occur

diag debug enable  
diag debug app authd -1  
allows you to debug FSSO events as the occur

```
FortiGate-VM64-2 (global) # diag debug app authd -1

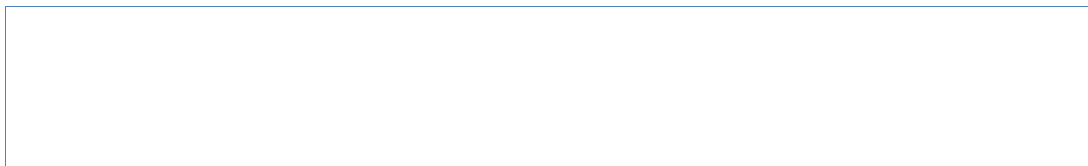
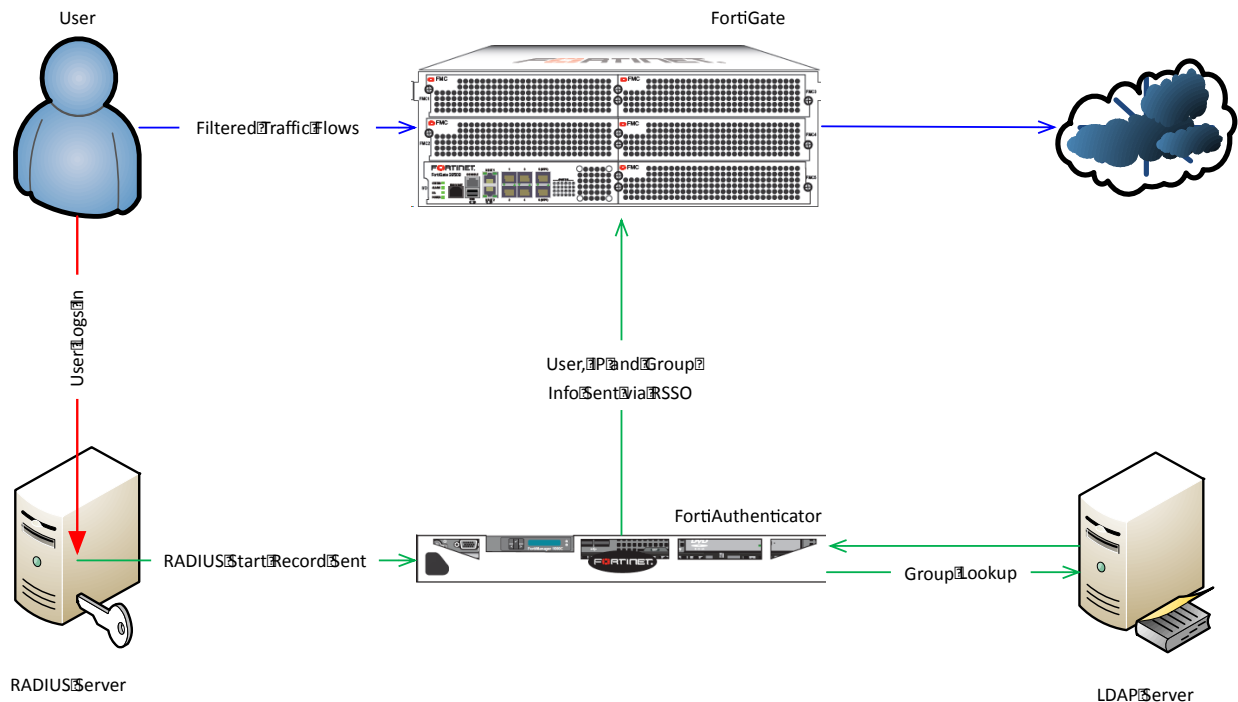
FortiGate-VM64-2 (global) # message_loop: checking timeouts
_event_read[FAC]: received heartbeat 0
message_loop: checking timeouts
_process_logon[FAC]: FTNTUNRESTRICTED(172.16.245.10) logged on with session id(
), port_range_sz=0
_process_logon-883: can not find such a user, try to add it
message_loop: checking timeouts
authd_admin.c:636 authd_admin_read: called
message_loop: checking timeouts
_event_read[FAC]: received heartbeat 0
message_loop: checking timeouts
message_loop: checking timeouts
_event_read[FAC]: received heartbeat 0
message_loop: checking timeouts
[fsae_db_logoff_user:453]: vfid 0, ip 172.16.245.10, FTNTUNRESTRICTED, sesion i
(0),port_range_sz(0)
[authd_fp_notify_logoff:251]: vfid 0, ip 172.16.245.10, id 0
_process_logoff[FAC]: FTNTUNRESTRICTED logged off
message_loop: checking timeouts
authd_admin.c:636 authd_admin_read: called
authd_del_auth_path: src_ip = af510ac, vd = root
Unknown sequence: 0af510ac
message_loop: checking timeouts
_process_logon[FAC]: FTNTRESTRICTED(172.16.245.12) logged on with session id(0)
port_range_sz=0
_process_logon-883: can not find such a user, try to add it
message_loop: checking timeouts
authd_admin.c:636 authd_admin_read: called
message_loop: checking timeouts
_event_read[FAC]: received heartbeat 0
message_loop: checking timeouts
```

## RADIUS Accounting via FortiAuthenticator RADIUS Accounting Proxy to Fortigate (FortiAuthenticator RSSO to RSSO)

FortiAuthenticator supports the use of RADIUS Start, Stop, and Interim Update messages to authenticate and manage active users transparently. It receives RADIUS accounting messages, Performs lookups against the LDAP server for Group Membership and then forwards the RADIUS message to the Fortigate RSSO agent.

This is useful when Group membership information is handled by Active Directory or the RADIUS server is business-critical IT infrastructure, limiting the changes that can be made to the server configuration.

Diagram





## FortiAuthenticator Steps and related CLI / Configuration Example

### Step 1 – Configure FortiAuthenticator as a RADIUS Accounting Proxy

Figure 23 – Configure Remote Auth Server

The screenshot shows the FortiAuthenticator web interface. The left sidebar is expanded to 'Authentication' > 'Remote Auth. Servers' > 'Edit Remote LDAP Server'. The main panel is titled 'Edit Remote LDAP Server'. It contains several sections:

- Name:** FTNT-AD
- Server name/IP:** 172.16.248.12, **Port:** 389
- Base distinguished name:** DC=ftnt,DC=local
- Bind type:** Simple (selected), Regular
- Username:** cn=Administrator,cn=Users,dc=ftnt,dc=local, **Password:** [masked]
- User object class:** person
- Username attribute:** sAMAccountName
- Group membership attribute:** memberOf
- Secure Connection:** ☐ Enable
- Windows Active Directory Domain Authentication:** ☒ Enable
  - Kerberos realm name:** FTNTLOCAL
  - Domain NetBIOS name:** FTNT
  - FortiAuthenticator NetBIOS name:** FortiAuthentic
  - Administrator username:** ftntAdministrator
  - Administrator password:** [masked]
- Remote LDAP Users:** A table with columns Username, Token, and Actions. It lists three users: ftntservices, ftntrestricted, and ftntuser. Each user has a red 'X' icon in the Actions column.

At the bottom, there are 'OK' and 'Cancel' buttons.

### Step 2 – Enable RADIUS Accounting SSO Clients

Figure 24 – Enable RADIUS accounting SSO Clients

The screenshot shows the FortiAuthenticator web interface. The left sidebar is expanded to 'Authentication' > 'Fortinet SSO Methods' > 'SSO' > 'General'. The main panel is titled 'Edit SSO Configuration'. It contains several sections:

- FortiGate:**
  - Listening port:** 8000
  - Login expiry:** 480 minutes
  - ☐ Enable authentication
- Fortinet Single Sign-On (FSSO):**
  - Maximum concurrent user sessions:** 0 (Configure Per User/Group)
  - Log level:** Debug
  - ☒ Enable Windows Active Directory domain controller polling
  - ☒ Enable RADIUS Accounting SSO clients (indicated by a red arrow)
  - ☒ Enable FortiClient SSO Mobility Agent Service
  - FortiClient listening port:** 8001
  - ☐ Enable authentication
  - Keep-alive interval:** 5 minutes (1-60)
  - Idle timeout:** 10 minutes
  - ☒ Enable NTLM
  - NTLM authentication expiry:** 480 minutes (1-10000)
  - ☒ Enable hierarchical FSSO tiering
  - Collector listening port:** 8002
  - ☒ Enable DC/TS Agent Clients
  - DC/TS Agent listening port:** 8003
  - ☒ Restrict auto-discovered domain controllers to configured domain controllers
  - ☒ Enable Windows Active Directory workstation IP verification
  - ☒ Enable IP change detection via DNS lookup
- Restart SSO service** button



## Step 3 – Create a new Accounting Proxy source

Figure 25 – Create a new Accounting Proxy Source

The screenshot shows the FortiAuthenticator web interface. The left sidebar is under 'System' > 'Authentication' > 'Fortinet SSO Methods' > 'Accounting Proxy' > 'Sources'. The main panel is titled 'Edit RADIUS Accounting Proxy Source'. It contains the following fields:

- Name: Win2k8AD
- Source name/IP: 172.16.245.12
- Secret: (masked with dots)
- Description: (empty)

At the bottom of the main panel are 'OK' and 'Cancel' buttons.

This information would be the RADIUS server.

## Step 4 – Create a new Accounting Proxy Create a new Rule Set

Figure 26 – Create a new Rule Set

The screenshot shows the FortiAuthenticator web interface. The left sidebar is under 'System' > 'Authentication' > 'Fortinet SSO Methods' > 'Accounting Proxy' > 'Rule Sets'. The main panel is titled 'Edit Rule Set'. It contains the following fields and sections:

- Name: RSSO
- Description: (empty)
- Rules section:
  - Rule: Add User-Name
  - Action: Add
  - Attribute: User-Name [Browse]
  - Value type: Group names
  - Username attribute: User-Name [Browse]
  - Remote LDAP: FTNT-AD (172.16.245.12:389)
  - Description: Add attribute "User-Name" containing "Group names" from group membership of "User-Name" attribute on remote LDAP server "FTNT-AD (172.16.245.12:389)"
  - + Add another Rule

At the bottom of the main panel are 'OK' and 'Cancel' buttons.

Select Action "Add" for a new attribute

Select Action "Modify" to translate an existent attribute

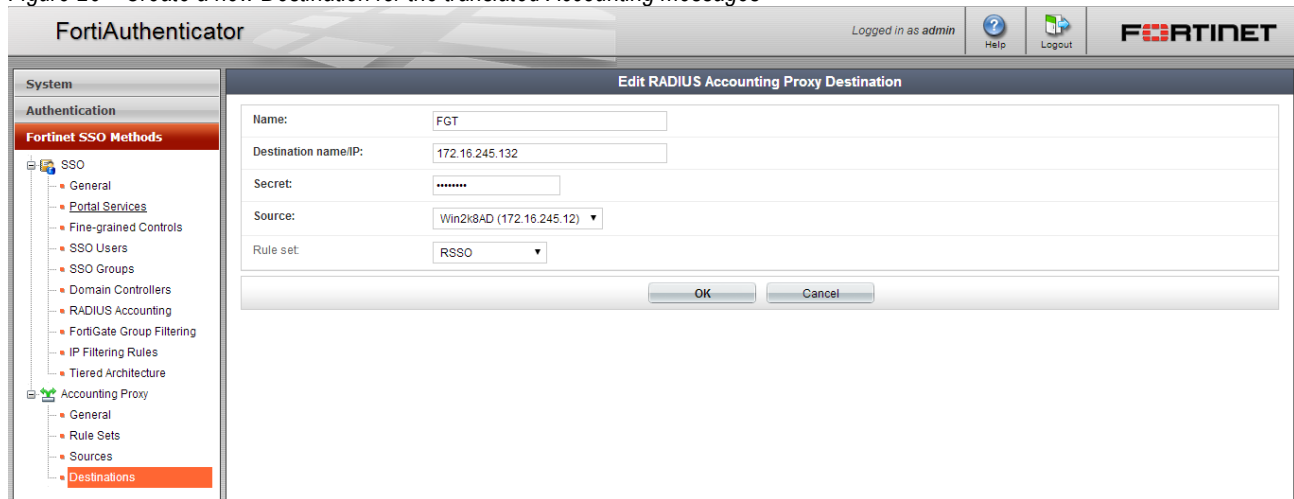
The attribute User-name is what the FortiAutheticator uses to parse group membership info from the LDAP Server.

The Value type is what we want FortiAuthenticator to add to the Accounting messages it forwards to the Fortigate. To add the user's group membership info select Group names.

Select the LDAP server that the FortiAuthenticator will run the group membership query on.

## Step 5 – Create a New Destination

Figure 26 – Create a new Destination for the translated Accounting messages



The screenshot shows the FortiAuthenticator web interface. The left sidebar contains a tree view with the following structure:

- System
  - Authentication
    - Fortinet SSO Methods**
      - SSO
        - General
        - Portal Services
        - Fine-grained Controls
        - SSO Users
        - SSO Groups
        - Domain Controllers
        - RADIUS Accounting
        - FortiGate Group Filtering
        - IP Filtering Rules
        - Tiered Architecture
      - Accounting Proxy
        - General
        - Rule Sets
        - Sources
        - Destinations**

The main content area is titled "Edit RADIUS Accounting Proxy Destination". It contains the following fields:

- Name: FGT
- Destination name/IP: 172.16.245.132
- Secret: .....
- Source: Win2k8AD (172.16.245.12) ▼
- Rule set: RSSO ▼

At the bottom of the form are "OK" and "Cancel" buttons.

This is the target for the translated Accounting message. Usually this is the Fortigate you wish to send the accounting message to but it can be any RADIUS Server configure to listen for Accounting messages.

Make certain you assign the rule set and source correctly.

## FortiGate Steps and related CLI / Configuration Example

Configuration and debugging on the Fortigate is the same as what is describe at the beginning of this document under **RADIUS Accounting Direct to Fortigate (Fortigate RSSO)**.

## Related Information

FortiOS and FortiGate Technical Documentation

<http://docs.fortinet.com/fgt.html>

Fortinet Knowledge Base

<http://kb.fortinet.com/>

FortiGate appliances

<http://www.fortinet.com/products/fortigate/>

FortiAuthenticator Technical Documentation

<http://docs-legacy.fortinet.com/fauth.html>

Copyright© 2011 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions. Network variables, different network environments and other conditions may affect performance results, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding contract with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Certain Fortinet products are licensed under U.S. Patent No. 5,623,600.